UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/746,604	12/22/2000	Geoffrey George Sweeney	11938/1	1011

26646 7590 10/19/2005

KENYON & KENYON
ONE BROADWAY
NEW YORK, NY 10004

EXAMINER	
WILLETT, STEPHAN F	
ART UNIT	PAPER NUMBER
2142	

DATE MAILED: 10/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/746,604	SWEENEY ET AL.	
	Examiner	Art Unit	
	Stephan F. Willett	2142	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 September 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-55* is/are pending in the application.

4a) Of the above claim(s) *4,25,45 and 47-52* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3, 5-24, 26-44, 46, 53-55* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *9/13/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC 102

1. The following is a quotation of the appropriate paragraphs of 35 U. S.C. 102(e) that form the basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-3, 5-24, 26-44, 46, 53-55 are rejected under 35 U.S.C. 102(e) as being anticipated by Proctor with Patent Number 6,530,024.

1. Regarding claim(s) 1, 22, 43, 53-55, Proctor teaches monitoring[auditing] a set of data[activities of a user] on said at least one system[user], col. 6, lines 11-12. Proctor teaches recording[logging] said event data[gathered data] in a database[log], col. 6, lines 49-50. Proctor teaches interrogating[analyzing] said database to thereby select alert event data[breaches] from said set of event data according to a predefined set of rules[detection policy], col. 6, lines 53-62. Proctor teaches reading said alert data and issuing an appropriate action[security response] due to said generated event, col. 6, lines 66-67, said action issued according to said predefined set of rules, col. 10, lines 54-56.

2. Regarding claim(s) 2, 23, Proctor teaches said action response occurs in real-time[shutting down] as a user interacts with said computing system, col. 7, lines 5-9.

3. Regarding claim(s) 3, 24, 44, Proctor teaches issuing said action response to said at least one computer system to prevent further interaction[logging off] of said user with said computing system, col. 7, lines 5-9.

4. Regarding claim(s) 5, 26, Proctor teaches said set of event data is monitored from the interaction of one or more users interaction with one or more computers on the network, col. 8, lines 45-47.

5. Regarding claim(s) 6, 27, Proctor teaches said monitored set of event data is monitored from a number of sources on said computer network, such as the application program layer, the transport layer, security layer, or operating system, col. 7, lines 48-50.

6. Regarding claim(s) 7, 28, Proctor teaches said application program layer includes enterprise resource planning, col. 1, lines 50-54.

7. Regarding claim(s) 8, 29, Proctor teaches said operating system includes a database application server, col. 8, lines 10-11.

8. Regarding claim(s) 9, 30, Proctor teaches said security layer includes firewalls, col. 8, lines 9-11.

9. Regarding claim(s) 10-11, 31-32, 46, Proctor teaches permitting an authorized user to interactively define said set of rules in step (c) using a GUI[screen], col. 9, lines 40-43.

10. Regarding claim(s) 12, 33, Proctor teaches said GUI is a web browser such as on the Internet, col. 18, lines 1-2.

11. Regarding claim(s) 13, 34, Proctor teaches determining said action response based upon said pre-defined set of rules and based upon a weighting factor[increased audit, security posture]

applied to recorded historical outcomes for monitored events[complete record], col. 7, lines 15-40,; col. 12, lines 35-41; col. 16, lines 32-42.

12. Regarding claim(s) 14, 35, Proctor teaches one or more agent program are provided on at least on computer of said computer system to thereby monitor said set of event data, col. 6, lines 32-33.

13. Regarding claim(s) 15, 36, Proctor teaches event data is recorded in a relational database[reduced audit records], col. 16, lines 52-58.

14. Regarding claim(s) 16-17, 37-28, Proctor teaches event data is assigned a unique log identifier[fields] in said database to identify the record of each event to correlate events, col. 16, lines 15-18.

15. Regarding claim(s) 18, 39, Proctor teaches a report is generated to report said recorded set of event data, col. 14, lines 62-63; col. 16, lines 57-58.

16. Regarding claim(s) 19, 40, Proctor teaches said appropriate action is a message sent to a network administrator, col. 10, lines 37-38.

17. Regarding claim(s) 20, 41, Proctor teaches said appropriate action is a message sent to an authorized person, col. 14, lines 55-57.

18. Regarding claim(s) 21, 42, Proctor teaches said message is of the type email, col. 10, lines 39-42.

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure is disclosed in the Notice of References Cited. A close review of the references is

suggested. The other references cited teach numerous other ways to monitor networks for relevant events, thus a close review of them is suggested.

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Stephan Willett whose telephone number is (571) 272-3890. The examiner can normally be reached Monday through Friday from 8:00 AM to 6:00 PM.

5. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jack Harvey, can be reached on (571) 272-3896. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

6. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

sfw

October 17, 2005

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER